UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/613,284	07/10/2000	David William Kravitz	1999-33	9794

23823 7590 03/01/2004

Digital Video Express, LP
1408 BAYSHIRE LANE
Herndon, VA 20170

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	4

DATE MAILED: 03/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/613,284	KRAVITZ ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in respect to applicants' application serial no. 09/613,284 filed on 7/10/2000.

Specification

2. The disclosure is objected to because of the following informalities:

On page 18, lines 12 and 20, the phrases "electronic book mode (ECB)" and "cipher blocking mode (CBC)" appear to be typographical errors.

Appropriate correction is required.

On page 18, line 5, the term "unencodeded" appears to b a typographical errors.

Claim Objections

3. Claims 2-12 are objected to because of the following informalities:

The acronyms should be spelled out to avoid confusion with other claim characters. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-12 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are:

In respect to claim 2, Cipher block chaining mode (CBC) is well known in the art, however, it is unclear what CBC' mode is encompassed.

In respect to claims 3-12, the claim limitations contain the language of the rejected claim 2. Therefore claims 3-12 are rejected based on the similar rationale.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1 and 13-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Enichen et al. (U.S. Patent No. 6,333,983).

In respect to claim 1, Enichen discloses an apparatus for key management comprising:

(a) a multitude of key registers, said multitude of key registers having a hierarchy with levels; (b) a multitude of type fields, wherein each type field is associated

with a key register (see col. 5, lines 3-15); (c) a key management controller, said key management controller having a multitude of modes; (d) at least one initialization vector (see col. 3, line 62-col. 4, line 11);

(e) key management algorithms (see col. 5, lines 3-14); and

(f) key management functions; wherein said mode is determined by the hierarchical level of the key register, and the key management algorithm used is determined by the key management function being used and said mode (see col. 5, lines 3-14 and col. 6, lines 22-61).

In respect to claim 13, Enichen discloses a method for generating an encoded value having a first encoded value part and a second encoded value part from an unencoded value having a first unencoded value part and a second unencoded value part, comprising the steps of:

(a) obtaining an initialization vector;

(b) generating the first encoded value part by:

(i) generating a first result by encrypting the first unencoded value part;

(ii) generating a second result by performing an exclusive or operation on the first result and the second unencoded value part;

(iii) generating a third result by performing an exclusive or operation on the second result and the initialization vector;

(iv) generating a fourth result by encrypting the third result;

(v) generating a fifth result by performing an exclusive or operation on the fourth result and the first unencoded value part; and

(vi) encrypting the fifth result; and

(c) generating the second encoded value part by encrypting the second result (see col. 3, line 61-11, cipher block chaining mode inherently teaches all the above enciphered steps).

In respect to claim 14, Enichen discloses the method according to claim 13, wherein said step of obtaining an initialization vector further includes the steps of:

(a) determining a hierarchical level for the encoded value; and

(b) obtaining the initialization vector determined by the hierarchical level (see col. 3, line 60-col. 4, line 10 and col. 5, lines 3-14).

In respect to claim 15, Enichen discloses the method for generating an unencoded value having a first unencoded value part and a second unencoded value part from an encoded value having a first encoded value part and a second encoded value part, comprising the steps of :

(a) obtaining an initialization vector:,

(b) generating the first unencoded value part by:

(i) generating a first result by decrypting the second encoded value part;

(ii) generating a second result by performing an exclusive or operation on the first result and the initialization vector;

(iii) generating a third result by encrypting the second result;

(iv) generating a fourth result by decrypting the second encoded value part; and

(v) performing an exclusive or operation on the third result and the fourth result;

(c) generating the second unencoded value part by:

(i) generating a fifth result by encrypting the first unencoded value part; and

(ii) generating a sixth result by decrypting the second encoded value part; and

(d) performing an exclusive or operation on the fifth result and the sixth result (see col. 4, lines 11-19, ciphered block chaining mode inherently teaches all the above deciphered steps).

In respect to claim 16, method according to claim 15, wherein said step of obtaining an initialization vector further includes the steps of

(a) determining a hierarchical level for the encoded value; and

(b) obtaining the initialization vector determined by the hierarchical level (see col. col. 4, line 11-20 and col. 5, lines 3-14).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Markham discloses a scalable key agile cryptography.

-Butter et al. Disclose a system for translating encrypted data.

-Matyas, Jr. et al. Disclose method and apparatus for cryptographically transforming an input block into an output block.

-Dabbish et al. Disclose a method and system for hierarchical key access and recovery.

-Lynn et al. Disclose a method and apparatus for variable-overhead cached encryption.

-Gilley discloses an apparatus for and method of overhead reduction in a block cipher.

-Perlman et al. Disclose a system and method for deriving an appropriate initialization vector for secure communications.

-Markandey et al. Disclose a data protection system.

Foster et al. Disclose a hierarchical key management system.

-Sudia et al. Disclose an electronic cryptographic packing.

-Shibata discloses a ciphering device and method in facsimile.

-Bellare discloses a method for data encryption/decryption using cipher block chaining (CBC) and message authentication codes (MAC).

Bruce Schneier discloses in chapter 9 different algorithm types and modes.

-Lu et al. Disclose enhanced protocols for hierarchical encryption key management for secure communication in Internet environment.

-Shigeta et al. Disclose a fine-grained protection mechanism in object based operating systems.

-Stubblebine et al. Disclose on message integrity in cryptographic protocols.

-Coppersmith et al. disclose attacks on MacDAC algorithm.

-Hellman discloses a cryptoanalytic time-memory tradeoff.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

February 17, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137